Find hidden files and directories

TLDR

```
 # Dirb
dirb https://192.168.1.101

# Gobuster - remove relevant responde codes (403 for example)
gobuster -u http://192.168.1.101 -w /usr/share/seclists/Discovery/Web_Content/common.txt -s '200,204,301,302,307,403,500' -e
```

About

There is essentially no way for a user to know which files are found in which directories on a web-server, unless the whole server has directory listing by default. However, if you go directly to the page it will be shown. So what the attacker can do is to brute force hidden files and directories. Just test a bunch of them. There are several tools for doing this. The attack is of course very noisy and will show up fast in the logs.

Dirb

This is a really easy tool to use:

```
dirb http://target.com
```

Dirbuster

It is a GUI You start it with:

```
dirbuster
```

OWASP ZAP

Insert your target. Add it to the context Click the plus-sign Click on Forced Browse

Wfuzz

You can find the manual by typing:

```
wfuzz -h
```

```
wfuzz -c -z file,/root/.ZAP/fuzzers/dirbuster/directory-list-2.3-big.txt --sc 200 http://pegasus.dev:8088/FUZZ.php
```

Gobuster

```
 # Gobuster - remove relevant responde codes (403 for example)
gobuster -u http://192.168.1.101 -w /usr/share/seclists/Discovery/Web_Content/common.txt -s '200,204,301,302,307,403,500' -e
```

WAF - Web application firewall

It might be that dirb shows you 403 errors, instead of the expected 404. This might mean that there is a WAF protecting the site. To get around it we might have to change our request header to it looks more like a normal request.

```
dirb http://target.com -a "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36
```